The Testimony of

Harris N. Miller,

President

Information Technology Association of America

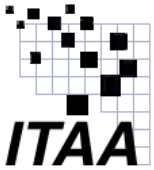
Before

The Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

Committee on Homeland Security

On H.R. 285, the Department of Homeland Security Cybersecurity Enhancement Act of 2005

April 20, 2005



Introduction

I am Harris N. Miller, President of the Information Technology Association of America (ITAA), representing over 380 member companies in the information technology (IT) industry - the enablers of the information economy. Our members are located in every state in the United States, and range from the smallest IT start-ups to industry leaders in the software, services, systems integration, telecommunications, Internet, and computer consulting fields. These firms are listed on the ITAA website at www.itaa.org.

I appreciate this Subommittee taking time from its very busy schedule to hold this hearing today on the need to elevate the issue of cyber security within the Department of Homeland Security (DHS) by creating an Assistant Secretary for Cyber Security. The constant attention by this Committee to the importance of cyber security in protecting our nation against terrorism is greatly appreciated by my members and all IT customers, whether they be individuals or companies.

After a lull in major network exploits, we have seen the issues of information security and critical infrastructure protection spring back into the news with the recent data breaches experienced by data brokers, database companies, universities, payroll processors and other types of organizations. As the development and adoption of electronic commerce evolves, the issue of "trust" becomes increasingly important. Businesses, government and citizens alike must trust the security of their information and the identity of the person or company on the other end. They must know the systems they are using are reliable. Events that shake this trust—whether real or perceived—pose a threat to the development of electronic commerce and the growth of the U.S. economy.

ITAA has played a major role in addressing the numerous issues of enhanced information security and cyber crime prevention. Our information security program dates back to 1999, with active participation from 250 IT companies. Since that time, along with many other accomplishments, ITAA has been proud to serve as a co-founder of the National Cyber Security Partnership, to chair the Partnership for Critical Infrastructure Protection, to co-found the National Cyber Security Alliance and the IT Information Sharing and Analysis Center (IT-ISAC) and to act as Sector Coordinator for the IT industry under Homeland Security Presidential Directive 7.

Why the U.S. Needs an Assistant Secretary for Cyber Security

Since the creation of the Department of Homeland Security, the Congress has become increasingly aware of the enormously complex challenges related to cyber security. The result is overwhelming bipartisan support in the committees of jurisdiction for a robust National Cyber Security Division (NCSD) to meet the broad challenges posed in the 2003 President's National Strategy to Secure Cyberspace. These challenges include creating and managing: a national cyber response system; a national program to reduce cyber security threats and vulnerabilities; a national cyber awareness and training program; and programs of coordination among federal, state and local governments, as well as with the private sector and with international partners.

ITAA, too, has been for several years advocating the need for a senior cyber security executive within the Federal government to help coordinate national cyber security policy among all industry, government and private sector stakeholders. We were the first organization to call for the creation of a cyber security "czar," and were very pleased that first President Clinton, by holding a White House meeting on cyber security in early 2000, and then President Bush, by establishing a cyber security advisor in the White House at the beginning of his term, each showed great leadership. But since the creation of the Department of Homeland Security, and the effective organizational demotion of the cyber security position, our concerns about Executive Branch leadership have returned.

Given strong bipartisan calls within Congress for a more robust NCSD capable of pulling together and coordinating among diverse entities within both government and the private sector, we feel very strongly that an Assistant Secretary position leading the NCSD is needed to meet the growing public administration, resource and policy challenges related to cyber security. This means coordinating closely with, but outside of, the Infrastructure Protection Division. When DHS was created, the decision was made to subsume cyber security coordination and outreach functions under an Assistant Secretary for Infrastructure Protection, on the premise that the integration of physical security and cyber security is better managed by one person, and that cyber security is only one component of physical security.

Our view, on the contrary, is that integration is best managed by two individuals, each experts in their respective fields, with a commitment to coordinating physical and cyber security where they are interrelated, with neither vital function subordinated to the other. It is clear that all of the nation's critical infrastructures, including water, chemicals, transportation, energy, financial services, health care, and others, rely significantly on computer networks to deliver the services that maintain our safety and national economy. It, therefore, is incumbent on the owners and operators of those critical infrastructures to manage improvements in the security of their information systems and to have a senior individual within the government, with effective influence and budget authority, who can coordinate collaborative efforts across critical infrastructure sectors and with state and local governments.

The NCSD has indeed made some progress; we applaud the valiant efforts of the former director and the current acting director and their creative and dedicated staff. But the current integration of cyber security and physical security is not working. As the IT Sector Coordinator, co-founder of the National Cyber Security Partnership and Chair of the Partnership for Critical Infrastructure Security – the cross-sectoral council of Federally-designated sector coordinators -- ITAA has witnessed the growing demands the Congress has placed on the NCSD to implement policies consistent with and beyond the President's National Strategy to Secure Cyberspace. ITAA also has experienced ongoing frustration with the confusion in the NCSD and its unrealized potential.

Indeed, the President's National Strategy is not being implemented as quickly and fully as it should, in large part, we believe, because the current organizational structure at DHS allows cyber security priorities to be marginalized against other physical security activities considered to have higher priority. Good management is always about allocating resources to the highest priorities set by both the Department and Congress, but too often the cyber security function has

suffered from missteps, and an increasing inability to meet the growing challenges that have been identified by Congress, government entities and the private sector.

Among them*:*

- DHS took several months to provide formal response to major private sector recommendations emerging from the December 2003 National Cyber Security Summit (see www.cyberpartnership.org), conducted in partnership with DHS and Secretary Ridge and designed to act on the President's National Strategy;

- A major "Partner Program" conference scheduled last year with industry and DHS was abruptly cancelled days before the event without explanation;

- The development of implementing regulations under the Homeland Security Act to protect critical infrastructure information (PCII) voluntarily submitted by private sector entities fails to facilitate information flows – as the law intended -- from the private sector custodians of cyber security early warning, analysis, and forensics -- to DHS. The IT-ISAC, for example, has submitted no critical cyber security information to DHS under this program, because the prescribed process does not reflect the realities of information management and proprietary business information within the private sector;

- DHS attempts to reorganize the private-sector "Sector Coordinator" and ISAC structures under Homeland Security Presidential Directive 7 proceeded against the counsel of several critical infrastructure representatives whose views may have been better reflected in this DHS initiative had they been heard at a more senior political level – such as an Assistant Secretary -- with guiding authority over staff;

- NCSD's cyber security R&D budget authority remains low and ineffectual. A division with an Assistant Secretary at the helm would likely command more resources; and

- It will not be until November of 2005 before we have a full cyber threat and attack exercise as a component of the DHS/industry critical infrastructure protection/emergency response exercises in the TOPOFF series, despite the real and identified threat of a coordinated physical/cyber attack on one or more of our critical infrastructures

The resulting bipartisan proposal within the Intelligence Reform bill to authorize the creation of an Assistant Secretary for Cyber Security underscores Congressional demands for a *confirmable* position of increased leadership within DHS that reflects the need for greater accountability to Congress.

Congressional Leadership

Last year, an amendment in the 9/11 bill creating the Assistant Secretary position was removed because of confusion during 11th hour negotiations. What was clear, however, was a White House position of "no objection" to the bill. Administrations as a matter of principle object to Congressional micromanagement of the President's organizational prerogatives. The official

White House position of neutrality in this particular case, however, speaks volumes, in our view, about the level of support within the White House for an improvement in the functioning of the cyber security activities of DHS.

The House Subcommittee on Cyber Security, Science and Research & Development underscored the need for an Assistant Secretary in its December 2004 Report on Cyber Security for the Homeland. The Subcommittee cited creation of this position as one of six "core" areas in its cyber security roadmap for the future.

We wholeheartedly applaud and support Congress in its efforts to provide the legislative impetus for this important position, and accordingly support H.R. 285.

While we believe the Assistant Secretary position is critical, it is not the only critical step remaining in this journey. The cyber security threat is constantly changing, and Congress has a role in assuring that adequate investment is made in safeguarding critical infrastructure and the U.S. economy from next generation threats.

Practical steps involve increasing appropriations for cyber security research as authorized in the Cyber Security Research and Development Act of 2002. More research is needed to improve information systems, and identify and reduce their vulnerabilities. Congress should also authorize and appropriate increases in the funding of NIST to support its Computer Security Division – a critical resource in the development of computer security standards and best practices for the private sector and government agencies.

Congress should also act to encourage the private sector to adopt more rigorous information security practices. For instance, lawmakers should explore whether, and under what circumstances, commercially viable information security insurance can be used as a market driver toward improvements in information security management in the enterprise. Other potentially productive strategies include considering limits on liability from cyber security breaches for companies that implement industry-agreed practices and creating economic incentives for information security technology procurement and implementation

Finally, the Senate should ratify the Council of Europe Convention on Cyber Crime, signed by the United States in November 2001.

Conclusions

No government executive will create single-handedly the policies or regulations to herald a new age of information security or to make cyber vulnerability a thing of the past. Logic tells us that we have turned a corner in our reliance on the Internet, and that along with the many blessings of the information economy and the knowledge society come the risks posed by the cyber delinquent, cyber criminal and cyber terrorist. A responsible government takes the steps necessary to maximize the benefits and to manage the risks appropriately.

Creating an Assistant Secretary for Cyber Security advances the cause of information security, introducing practical advantages and sending an important symbolic message. Much needs to be

done to improve the performance and to elevate the position of cyber security as an issue in the Administration, to coordinate information security across disparate government agencies, and to build the necessary bridges between the federal government and critical infrastructure industries. For far too long, the federal government's symbolic role in information security has gone begging—the "bully pulpit" stands empty. Consumers, small businesses and other organizations peg their response to various issues by the actions (or lack thereof) of policymakers. We believe that cyber security is one such issue.

In calling for the increased leadership that we believe an Assistant Secretary will bring to the goal of heightened cyber security, industry also stands ready to do its part—and the good news is that we have done much already. An ITAA-commissioned survey conducted by the University of Southern California's Institute for Critical Information Infrastructure Protection (ICIIP) at the Marshall School of Business identified 175 examples of cyber security enhancing products, services or activities from 65 responding organizations, including cross-sectoral and vertical industry groups and trade associations, multinational and owner-operated businesses, academic institutions, and professional societies. Intrusion detection and early warning networks, structures for information sharing, enhanced commercial products across an array of information security functionalities, guides, white papers, no-charge anti-virus protections and automatic software update capabilities are just some examples of the industry-led strides to raise the nation's cyber security profile.

The federal government faces a full agenda of cyber security issues. The challenges of providing critical infrastructure protection are formidable today and are likely to be even significant in the future. An Assistant Secretary for Cyber Security can make an important difference. We thank the Subcommittee for bringing this important issue to the attention of the American people.

Thank you very much.